

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

THOMAS B. WILNER, et al.,)	
)	
Plaintiffs,)	
)	
v.)	Civil Action No. 07-CIV-3883
)	
NATIONAL SECURITY AGENCY and)	
DEPARTMENT OF JUSTICE,)	
)	
)	
Defendants.)	
)	

(U) REDACTED SUPPLEMENTAL DECLARATION OF JOSEPH J. BRAND

I, Joseph J. Brand, declare as follows:

1. (U) I am the Associate Director, Community Integration, Policy and Records for the National Security Agency ("NSA" or the "Agency"). This declaration supplements my earlier declaration dated 18 March 2008, which among things, explained my role as a TOP SECRET classification authority, my responsibilities in processing requests made pursuant to the Freedom of Information Act, the origin and mission of NSA, the Terrorist Surveillance Program ("TSP"), and why NSA could not confirm publicly in any particular case whether or not any intelligence was collected pursuant to the TSP or the surveillance now authorized by the Foreign Intelligence Surveillance Court ("FISC") or, conversely, that no such collection occurred.

2. (U) The purpose of this declaration is to explain why operational details of the TSP such as those sought by the plaintiffs cannot be publicly disclosed. This information is currently and properly classified in accordance with E.O. 12958 - Classified National Security Information - , as amended, and is protected from disclosure by statute.

Additionally, certain information is further protected from disclosure based on the attorney-client privilege, the deliberative process privilege, and the attorney work product doctrine.

**(U) NSA'S WITHHOLDING OF INFORMATION PERTAINING TO
OPERATIONAL DETAILS**

3. (U) Plaintiffs seek information on policies, procedures, guidelines or practices for the interception of communications pursuant to the TSP. See Second Am. Compl. ¶

8. Plaintiffs seek the same information from Department of Justice ("DOJ"), and this declaration explains why the responsive information in both NSA's custody and control as well as the information referred to NSA from DOJ is properly exempt from disclosure under the FOIA. As set forth in detail below, I am confident, based on my knowledge of the TSP and my position as the Associate Director, Community Integration, Policy and Records, that all of the records responsive to plaintiffs' FOIA requests describe the NSA's operation of the TSP. Documents describing operational details related to the TSP are exempt from disclosure in their entirety based on Exemption One because the information is currently and properly classified in accordance with E.O. 12958, as amended; Exemption Three because the information is protected from disclosure by statute; and for certain information, Exemption Five because of the attorney-client privilege, the deliberative process privilege, and the attorney work product doctrine.

(U) ORIGIN AND MISSION OF NSA

4. (U) NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. See Executive Order 12333, Section 1.12(b). NSA's cryptologic mission has three functions: to collect, process, and disseminate SIGINT information for national foreign intelligence purposes; to conduct

information security activities; and to conduct operations security training for the United States Government.

5. (U) Signals intelligence is one of NSA's primary missions. NSA's SIGINT mission is to obtain information from foreign electromagnetic signals and to provide, frequently on a rapid response basis, reports derived from such information or data to national policy makers, combatant commanders, and the intelligence community of the United States Government. A primary SIGINT mission of NSA is to intercept communications in order to obtain foreign intelligence information necessary to the national defense, national security, or the conduct of the foreign affairs of the United States. The SIGINT collection mission of NSA provides national policy makers and the intelligence community with highly reliable foreign intelligence information.

6. (U) The Agency's SIGINT mission includes gathering intelligence from various sources and methods, which enable it to keep pace with challenging developments in communications technology. In the course of fulfilling its mission, NSA produces foreign intelligence and reports it to customers within the United States Government.

7. (U) There are two primary reasons for gathering and analyzing intelligence information. The first, and most important, is to gain the information required to direct U.S. resources as necessary to counter external threats. The second reason is to obtain the information necessary to direct the foreign policy of the United States. Information produced by SIGINT is relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; arms proliferation; terrorism; and foreign aspects of international narcotics trafficking. This information is often critical to the

formulation of U.S. foreign policy and the support of U.S. military operations around the world. Moreover, intelligence produced by NSA is often unobtainable by other means.

8. (U) NSA has developed a SIGINT collection network that acquires, among other things, foreign and international electronic communications. The technological infrastructure that supports NSA's foreign intelligence information collection network has taken years to develop at a substantial cost and untold human effort. It relies on sophisticated collection and processing technology.

9. (U) NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Further, SIGINT technology is both expensive and fragile. Public disclosure of either the capability to collect specific communications or the substance of the information itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing the intelligence collection techniques that are applied against targets around the world. Once alerted, SIGINT targets can implement measures to thwart continued SIGINT collection.

10. (U) Information obtained from intercepted foreign communications is called communications intelligence ("COMINT"). NSA's COMINT efforts constitute only part of the functions and activities of the Agency. A fundamental tenet of the COMINT process is that the identity of specific communications (commonly referred to as "targets"), the degree of success in exploiting these targets, and the vulnerability of particular foreign communications are all matters that must be maintained in strictest secrecy because of the fragile ability to exploit foreign communications. Disclosure of the identity of the targets, the ability to exploit those targets, or the vulnerability of

particular foreign communications would encourage countermeasures by the targets of NSA's COMINT efforts. If a target is successful in defeating a NSA intercept operation, all of the intelligence from that target is lost unless and until NSA can establish new and equivalent exploitation of that target's signals. If a source becomes unavailable, the military, national policymakers, combatant commanders, and the intelligence community must operate without the information the signals provided. Such losses are extremely harmful to the national security of the United States.

(U) THE TERRORIST SURVEILLANCE PROGRAM (TSP)

11. (U) Following the devastating attacks of September 11, 2001, the President of the United States authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The TSP was a targeted and focused program intended to help "connect the dots" between known and potential terrorists and their affiliates. In order for communications to be intercepted under the TSP, there was a requirement to have a reasonable basis to conclude that one party to the communication was located outside the United States and that one party to the communication was a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda or terrorism. Thus, the TSP program was an "early warning" system with one purpose: to detect and prevent another catastrophic attack on or within the United States.

12. (U) The TSP was a SIGINT program that was critical to the national security of the United States. The President publicly acknowledged the existence of the program on December 17, 2005. As the President has made clear, however, details about the TSP remain highly classified and subject to special access restrictions under the criteria set

forth in Executive Order 12958, as amended. Unauthorized disclosure of information regarding the TSP can be expected to cause exceptionally grave damage to the national security of the United States. Thus, pursuant to the criteria outlined in Executive Order 12958, as amended, information related to the TSP is classified TOP SECRET, and is subject to the special access and handling requirements reserved for "Sensitive Compartment Information," (SCI), because it involved or was derived from particularly sensitive intelligence sources and methods.

13. (U) NSA's SIGINT operations, including the TSP (the surveillance authorized by the President) or the surveillance now authorized by the FISC, are both sensitive and fragile. The critical intelligence information that is derived from NSA's SIGINT operations depends upon the collection of electronic communications, which can be easily compromised if targets are made aware of NSA capabilities and priorities. If an individual learns or suspects that his\her signals are or may be targeted by the NSA for collection, he\she may take steps to evade detection, to manipulate the information that NSA receives, or to implement other countermeasures aimed at undermining the NSA's operations. The resulting loss of intelligence from such a source deprives the U.S. of information critical to U.S. interests, such as the prevention of terrorist attacks.

14. (U) Congress has specifically recognized the inherent sensitivity of the SIGINT activities of the NSA; thus, Congress has passed statutes to protect the fragile nature of NSA's SIGINT efforts. These statutes recognize the vulnerability of signals intelligence to countermeasures of a foreign power or terrorist party and the significance of the loss of valuable foreign intelligence information to national policymakers, combatant commanders, and the intelligence community. These statutes are: Section 6 of

the National Security Agency Act of 1959 (codified at 50 U.S.C. § 402 note); Section 102A(i)(I) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1); and 18 U.S.C. § 798. Under these three statutes, NSA is specifically authorized to protect certain information concerning its activities, and its intelligence sources and methods, from public disclosure.

(U) NSA'S PROCESSING OF PLAINTIFFS' FOIA REQUEST

15. (U) As set forth in my prior declaration in this case and incorporated by reference here, see Brand Glomar Declaration ¶¶ 15-17 & attachments 1-4 thereto, NSA responded to plaintiffs January 18, 2006 FOIA request on February 26, 2008. The plaintiffs' request sought records pertaining to eight categories of information. I understand that only one item is at issue in this litigation, which is NSA's response to item three of Plaintiff's request, which was for "policies, procedures, guidelines or practices for the interception of communications pursuant to the previously described warrantless surveillance program."

16. (U) The TSP was a highly classified and compartmented intelligence program as to which only a relatively small number of individuals have been cleared for access. NSA interpreted Plaintiffs' request for "policies, procedures, guidelines or practices for the interception of communications" to pertain to documents responsive to NSA's content collection of international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations, which is the presidentially authorized program that has been publicly acknowledged as the TSP.

17. [REDACTED]

18. [REDACTED]

19. (U) In response to Plaintiff's FOIA request for policies, procedures, guidelines or practices for the interception of communications pursuant to the TSP, the Agency searched for and located responsive records in NSA organizations that managed and operated the TSP. Accordingly, I am confident that the Agency's search was reasonable, and this search located the records that were responsive to Plaintiffs' FOIA request.

(U) OPERATIONAL DETAILS ON THE TSP ARE CLASSIFIED AND PROTECTED FROM DISCLOSURE BASED ON FOIA EXEMPTION ONE

20. (U) Section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of the national defense or foreign policy and are in fact properly classified pursuant to such Executive Order. The current Executive Order, which establishes such criteria, is Executive Order 12958, 60 Fed. Reg. 19825 (Apr. 17, 1995), as amended by Executive Order 13292, 68 Fed. Reg. 15315 (Mar. 25, 2003) (hereinafter "E.O. 12958, as amended").

21. (U) Executive Order 12958 Section 1.4 provides that information may not be considered for classification unless it falls within seven specifically enumerated categories of information. I have concluded that all records responsive to Plaintiffs' FOIA request pertain to information that meets the criteria for classification as set forth in Subparagraphs (c) and (g) of Section 1.4 of Executive Order 12958, as amended, which authorizes the classification of information concerning "intelligence activities (including special activities), intelligence sources or methods, or cryptology," and "vulnerabilities or

capabilities of systems, installations, infrastructures, projects, plans, or protection systems relating to national security, which includes defense against transnational terrorism.”

22. (U) Additionally, the responsive records are currently and properly classified TOP SECRET pursuant to Executive Order 12958, as amended, section 1.2.(1), because their disclosure reasonably could be expected to cause exceptionally grave damage to the national security. Further, the information is subject to Sensitive Compartmented Information (SCI) control systems, which requires special access and handling restrictions. Accordingly, since I reviewed the responsive documents for classification under the current classification Executive Order, Executive Order 12958, as amended, and determined that they are currently and properly classified TOP SECRET-SCI, the documents in question are properly exempt from disclosure pursuant to FOIA Exemption One.

23. (U) Any disclosure of information responsive to Plaintiffs’ request would reveal details about the operation of the TSP and the surveillance now authorized by the FISC, and its strengths and vulnerabilities, which could have the effect of compromising the effectiveness of NSA’s SIGINT activities and undermining its goal of detecting and preventing the next terrorist attack on the United States. Disclosure of policies, procedures, guidelines or practices pertaining to the collection of communications under the TSP would allow our adversaries to determine which methods of communications are vulnerable for collection, what activities or operations may trigger NSA collection efforts, and could reveal to the enemy which persons have been identified as, or linked to, a potential threat. Such information is invaluable to the enemy – the disclosures sought by the plaintiffs will alert the enemy whether or not their operations may have been

compromised and this would enable them to adopt strategies to circumvent surveillance and to otherwise evade detection if their communications were compromised. Such disclosures would also inform the enemy which communications and operations could be evading NSA's collections efforts, and this would result in their increased use of particular means or technique of communication. These disclosures would do immeasurable damage to the national security of the United States.

24. (U) Further, the disclosure of information about the operational details of the TSP would reveal information about NSA's success or lack of success in implementing the TSP. The disclosure of NSA's ability or lack of ability to access or monitor an individual's communications reveals U.S. intelligence community's capabilities, priorities, and activities. The disclosure of this information could reasonably be expected to cause exceptionally grave damage to the national security because it gives the nation's adversaries information about the nature and frequency of the Government's use of specific techniques that could assist them in undermining the NSA and the intelligence community's national security mission.

25. (U) Thus, disclosing any operational details of the TSP, to include, but not limited to the policies, procedure, guidelines or practices regarding the collection of communications, would provide our adversaries with critical information about the capabilities and limitations of the NSA, such as the types of communications that may be susceptible to NSA detection. Our adversaries could exploit this information in order to conduct their international terrorist activities more securely, to the detriment of the national security of the United States. Accordingly, any operational details of the TSP are exempt from disclosure pursuant to Exemption 1 of the FOIA because the

information is currently and properly classified in accordance with Executive Order 12958, as amended.

**(U) OPERATIONAL DETAILS ON THE TSP ARE PROHIBITED FROM
DISCLOSURE BY STATUTE AND THUS EXEMPT FROM RELEASE BASED ON
FOIA EXEMPTION THREE**

26. (U) Section 552(b)(3) of the FOIA provides that the FOIA does not require the release of matters that are specifically exempted from disclosure by statute, provided that the relevant statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or establishes particular criteria for withholding or refers to particular types of matter to be withheld. *See* 5 U.S.C. § 552(b)(3). Information about NSA's Signals Intelligence (SIGINT) efforts directly relates to the Agency's most core functions and activities. These functions and activities are protected from public disclosure by several statutes. Congress has passed these statutes to protect the fragile nature of NSA's SIGINT efforts, including, but not limited to, the existence and depth of signal intelligence-related analytical successes, weaknesses and exploitation techniques. These statutes recognize the vulnerability of signals intelligence to countermeasures by targets and the significance of the loss of valuable foreign intelligence information to national policymakers and the intelligence community.

27. (U) The first of these statutes is a statutory privilege unique to NSA. NSA's statutory privilege is set forth in section 6 of the National Security Agency Act of 1959, Public Law 86-36 (50 U.S.C. § 402 note). Section 6 of the NSA Act provides that **“[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of**

any information with respect to the activities thereof, . . . ” (emphasis added). By this language, Congress expressed its finding that disclosure of any information relating to NSA activities is potentially harmful to National Security. The courts have held that the protection provided by this statutory privilege is, by its very terms, absolute. *See, e.g., Linder v. NSA*, 94 F. 3d 693 (D.C. Cir. 1996). Section 6 states unequivocally that, notwithstanding any other law, including the FOIA, NSA cannot be compelled to disclose any information with respect to its activities. *See Hayden v. NSA*, 608 F.2d 1381 (D.C. Cir. 1979). Further, while in this case the harm would be very serious, NSA is not required to demonstrate specific harm to national security when invoking this statutory privilege, but only to show that the information relates to its activities. *Id.* To invoke this privilege, NSA must demonstrate only that the information sought to be protected falls within the scope of section 6. NSA’s functions and activities are therefore protected from disclosure regardless of whether or not the information is classified.

28. (U) The second applicable statute is 18 U.S.C. § 798. This statute prohibits the unauthorized disclosure of classified information (i) concerning the communications intelligence activities of the United States or (ii) obtained by the process of communication intelligence derived from the communications of any foreign government. The term “communications intelligence,” as defined by Section 798, means the procedures and methods used in the interception of communications and obtaining of information from such communications by other than the intended recipients.

29. (U) The third applicable statute is Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1), which states that the Director of National Intelligence shall protect intelligence sources and methods from

34. (U) The logic behind the deliberative process privilege is that by maintaining the confidentiality of the give-and-take that occurs among agency members in the formulation of policy, the deliberative process privilege encourages frank and open discussions of ideas, and hence, improves the decision making process. Similarly, the attorney-client privilege protects confidential communications between the agency and its attorneys, both within NSA and at other agencies, including at DOJ. This entire process would be harmed if participants could no longer expect confidentiality when engaging in internal discussions as attorneys may be concerned about providing full and frank advice over concerns that such advice would be publicly released. Accordingly, the Plaintiff's requested information is also exempt pursuant to Exemption 5 of the FOIA.

(U) CONCLUSION

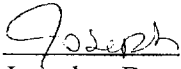
35. (U) In conclusion, NSA has properly invoked Exemptions 1, 3 and 5 of the FOIA for its withholding of the information discussed therein. Moreover, the responsive NSA information cannot be segregated so as to release any non-exempt information. The information contained in the responsive records, which is classified and protected from release by statute as set forth above, is so intertwined with additional information regarding the details of operation of the TSP that it cannot be segregated and released without compromising the national security of the United States. This is especially significant given the fact that NSA is the agency which operated the TSP. As such, even the release of general information about the TSP poses the substantial risk that our adversaries will be able to piece together sensitive information about how the program operates. For example, disclosing the dates on which documents were created, the subjects of TSP-related documents, or the volume of documents relating to the TSP

reveals information about the capabilities, scope and effectiveness of the program, which would be utilized by the enemy and allow them to plan their terrorist activities more securely. Accordingly, no segregable portion of the responsive documents may be disclosed.

36. (U) Finally, because of the highly sensitive nature of the information involved and the detailed information provided in this declaration, and because the program at issue, the TSP, was a NSA program, requiring NSA to produce an index of the particular documents withheld would be inappropriate. NSA has the fullest picture of procedures relating to the program and requiring from NSA such an index would require a description of documents that would reveal information so highly classified that few Agency officials have been provided with access to it; would require a description of potential documents the existence of which NSA has neither confirmed nor denied; and would itself reveal information specifically protected by FOIA Exemptions 1 and 3. See People for the American Way v. Nat'l Security Agency, 462 F. Supp. 2d 21, 27 and 30 (D.D.C. 2006); E.D. Edmunds v. FBI, 272 F. Supp. 2d. 35, 44 (D.D.C. 2003).

(U) I declare under of penalty of perjury that the foregoing is true and correct.

Signed this 1st day of May 2008

 B
Joseph B
Associate Director, Community
Integration, Policy and Records
National Security Agency